IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH AND SEIZURE OF:	)	
	)	Mag. No. 3:21-78 MJ
TCL Black TRAC Phone;	)	[UNDER SEAL]
TCL Black TRAC Phone with MicroSD Card;	)	
SanDisk MicroSD card adapter;	)	
Two (2) Square Scandisk MP3 players;	)	
MicroSD card adapter;	)	
Two (2) MicroSD card adapters;	)	
TRAC phone booklets; and	)	
Receipts and bill for TRAC phone.	)	

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

I, Robert E. Connelly, II, a Special Agent with Homeland Security Investigations (HSI), being duly sworn, depose and say:

INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the Pittsburgh, Pennsylvania Office. I have been so employed as a Special Agent since November 2001. As part of my duties as an HSI Special Agent, I investigate criminal violations relating to high technology crime, cyber-crime, child exploitation and child pornography including violations pertaining to the illegal distribution, receipt, and possession of materials depicting the sexual exploitation of children in violation of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4)(B). I have received training in the area of child pornography and child exploitation investigations and have had the opportunity to observe and review numerous examples of such materials in a variety of electronic media. I have participated in and led numerous child pornography investigations. I have executed numerous search warrants

related to child pornography investigations. In this regard, I have reviewed extensive samples of child pornography, including videos, photographs, and digital reproductions of photographs or other print media.

2. This affidavit is made in support of an application for a warrant to seize the following items, which are currently being stored in secure evidence at the United States Probation Office for the Western District of Pennsylvania, and to search the electronic devices/electronic storage media: (1) a TCL Black TRAC Phone; (2) a TCL Black TRAC Phone with MicroSD card; (3) a SanDisk MicroSD card adapter, (4) Two (2) Square Scandisk MP3 players; (5) a MicroSD card adapter; (6) two (2) MicroSD card adapters; (7) TRAC phone booklets; and (8) receipts and bill for TRAC phone. Within this Affidavit your affiant will refer to these items as the "Subject Items."

3. I make this application pursuant to Rule 41 of the Federal Rules of Criminal Procedure. The purpose of this application is to seize evidence, fruits, and instrumentalities, more particularly described in Attachment B, of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), which makes it a crime for any person to knowingly receive or distribute or access with intent to view material that depicts minors engaged in sexually explicit conduct that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

4. Through my experience and training, I am aware that Title 18, United States Code, Section 2256 defines "minor", for purposes of Section 2252, as "any person under the age of eighteen years". Section 2256 also defines "sexually explicit conduct" for purposes of these sections as including: (a) genital-genital, oral-genital, anal-genital, and oral-anal sexual intercourse, whether between persons of the same or opposite sex; (b) bestiality; (c)

masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

5. The statements in this affidavit are based, in part, on information provided by witnesses and your affiant's investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4)(B) that are presently located within the Subject Items.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

6. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

7. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

8. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how

the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

9. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

FACTS AND CIRCUMSTANCES

10. Your affiant is participating in a child exploitation investigation of an individual named Kristian E. HELLER who, prior to his recent arrest, was residing at 291 Old Bedford Pike, Windber, Pennsylvania 15963.

11. Kristian HELLER is currently under federal supervised release as part of his sentence for Transportation of Material Depicting the Sexual Exploitation of a Minor, in violation of 18 U.S.C. 2252(a)(1), a Class C Felony. See, case number 3:05-cr-22.

12. HELLER was sentenced by United States District Judge Kim R. Gibson on October 20, 2008 to 97 months' imprisonment followed by 120 months' supervised release.

13. Special conditions of HELLER's supervised release included that he participate in sex offender treatment, be subject to computer/internet use restrictions, participate in polygraph examinations, and that he not possess child pornography materials, among others.

14. On December 22, 2016, the United States Probation Office filed a Petition for Show Cause Hearing alleging that, following a polygraph examination, HELLER admitted to possessing a USB drive that contained images of child pornography. According to HELLER (per the USPO), he possessed the device secretly and intentionally withheld that information from his probation officer and treatment provider. HELLER's alleged violations were for committing a new federal, state, or local crime; possessing child pornography; failing to answer truthfully questions asked by probation officer; and being unsuccessfully discharged from sex offender treatment due to violating treatment conditions.

15. On February 14, 2017, HELLER's supervised release was revoked. HELLER was sentenced to 9 months' imprisonment to be followed by recommencement of the balance of the original term of supervised release. New standard conditions of supervision and special conditions were added as part of the court's Amended Judgment.

16. HELLER served the sentence of imprisonment and recommenced supervised release on November 9, 2017.

17. On February 13, 2019, the USPO again filed a Petition for Warrant or Show Cause Hearing. This time, the USPO alleged that HELLER admitted to the probation officer that he failed to report for his polygraph exam as scheduled because he possessed internet-capable devices (a tablet and smartphone) which were not authorized. According to the USPO, the USPO obtained the smartphone, which contained a memory card. The device/storage media was forensically analyzed and found to contain suspected child pornography. Thus, the alleged violations committed by HELLER on this occasion were that he committed a new federal, state or local crime; possessed child pornography; used an electronic communication data storage device, to include a cellphone, to access child pornography; failed to provide the U.S. Probation Office with accurate information about his electronic communication/data storage devices; and failed to participate in sex offender treatment to include polygraphy testing. The Court issued an arrest warrant.

18. On November 14, 2019, HELLER admitted to the violations and his supervised release was revoked. HELLER was sentenced to the statutory maximum term of imprisonment—24 months'—to be followed by a new, 10-year term of supervised release under the same conditions previously-imposed in the Amended Judgment.

19. HELLER served his sentence of imprisonment and again commenced supervised release on November 2, 2020.

20. Thus, twice before HELLER's supervised release has been revoked due to similar patterns of noncompliance to include new criminal conduct relating to child pornography.

21. On April 20, 2021, HELLER completed a polygraph examination as part of his conditions of supervised release.

22. Prior to this polygraph examination HELLER admitted to his probation officer and polygrapher that he, HELLER, had done things he should not have done involving the Internet. During the pre-test interview with the polygrapher, HELLER admitted to the polygrapher that he purchased a smartphone several months ago and had used it to access the Internet, that he used the phone to access and view pornography and child pornography, that he had masturbated daily, and that he videotaped himself masturbating which he shared on the Internet.

23. HELLER was administered the polygraph exam and was not found to be deceptive during the polygraph exam.

24. With respect to the smartphone, HELLER told the probation officer and polygrapher that he had discarded it on the way to the polygraph exam and he informed the probation officer of the specific location where he had thrown the smartphone in the trash.

25. After the interview, probation officers conducted an authorized search of HELLER's vehicle, which yielded a USB converter. HELLER claimed that the device only contained music.

26. Probation officers then proceeded to the location where HELLER said he had discarded the smartphone in the trash (a Sheetz gas station located in Somerset). Located in the trash container indicated by HELLER were actually two smartphones. HELLER confirmed that both belonged to him but said that one smartphone was inaccessible.

27. Probation officers next proceeded to HELLER's residence and conducted a search of his bedroom. There they found 3 micro SD cards, USB cables/chargers, an Alcatel phone

charger, two MP3 players, receipts, and a bill for TRAC phone data and TRAC phone booklets, all of which were seized by probation secured into probation's evidence.

28. HELLER admitted to Probation Officer Brian Frycklund that there would be child pornography on both smartphones seized from the trash and on one of the micro SD cards seized from his bedroom.

29. On April 21, 2021, US Probation sent the electronic property seized from HELLER to the Probation Forensics Lab in the Eastern District of Missouri to be forensically-analyzed to determine if they contained any child sexual abuse material (CSAM).

30. On April 28, 2021, U.S. Probation informed the United States Attorney's office that a preliminary review of the devices resulted in the discovery of at least one image of child pornography on one of the smartphones.

31. On May 6, 2021, the US Probation Office informed the United States Attorney's Office that the evidence sent to the Forensics Lab in Missouri had been returned to their custody.

32. On May 7, 2021, your affiant reviewed an email from US Probation Officer Danylle Ford in which USPO Ford confirmed that CSAM was found on the two smartphones and the microSD card found in one of the TRAC phones. The forensics conducted on the other electronic devices did not yield the discovery of CSAM.

33. Your affiant is unaware of which forensic examination software/techniques were employed during the examination conducted by the US Probation Forensic group. Your affiant knows that certain forensic software/techniques may not result in the discovery of all CSAM on a particular device, e.g., certain software/techniques may not discover all files that have been deleted. Moreover, evidence of the federal criminal offenses described earlier within this

affidavit (18 U.S.C. §§ 2251 and 2252) is not limited to CSAM exclusively. For example, indicia of ownership of a particular device or a particular device's internet history can be just as valuable to the investigation of a suspected child pornography-related crime as the CSAM itself.

34. Therefore, although the USPO conducted a forensic examination of the devices and found that some did not contain CSAM, the absence of CSAM does not conclusively determine the absence of evidence of a child pornography offense.

35. The TCL Black TRAC Phone, TCL Black TRAC Phone with MicroSD card, SanDisk MicroSD card adapter, 2 Square Scandisk MP3 players, 1 MicroSD card adapter, 2 MicroSD card adapters, TRAC phone booklets, Receipts, and bill for TRAC phone are currently in the possession of U.S. Probation Office in Johnstown.

CONCLUSION

36. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code, Sections 2251(a)(1) and 2252(a)(2) will be located on or within the Subject Items.

37. Your Affiant, therefore, respectfully requests that the attached warrant for the Subject Items be issued authorizing the search and seizure of the items listed in Attachment A.

38. The above information is true and correct to the best of my knowledge, information and belief.

/s/ Robert E. Connelly, II
ROBERT E. CONNELLY
Special Agent, HSI

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 10th day of May 2021.

_____
HONORABLE KEITH A. PESTO
United States Magistrate Judge